5 因數分解

用埃氏篩來找尋質數，效率可以算得上是非常高，但假若要在給定範圍內找出質數，用埃氏篩的方法，每次都得從頭做起,亦需花上不少時間。是以很多人會選擇直接將數字進行分解。

將 n 分解，可以用試誤的方式,由 2,3,5,7,...等小於 $\sqrt{n}$ 的質數，逐一去除 n。 而坊間亦有不少檢驗整除性的簡捷方法。

5.1 整除性

以下爲常見的整除性檢定方法:

1. 若一個數末尾的數字爲 2,4,6,8,或 0, 這個數是 2 的倍數。
2. 若將某數的每個數位上的數字相加，若其和能爲 3 所整除，則這個數是 3 的倍數。
3. 若一個數末尾的數字爲 0 或 5, 這個數是 5 的倍數。
4. 若由某數的最高位的數字開始，依次交替地加減，若最終得出的結果爲 11 倍數，則這個數是 11 的倍數。

5.1.1 7 的整除性

判別一個數的整除性, 除了上述常見的方法外, 用截尾法可以設計出不同的判定整除性的方法, 以下展示 7 的整除性的判定方法：

1. 將原來的數字截去末端的數字，
2. 將由餘下的數字組成的數減去剛截去數字的 2 倍
3. 若確知所得的差能否被 7 整除,則停止,否則重複步驟 (1) 至 (3)。

例(1): 判定 12345 能否被 7 整除

1. 將原來的數字 12345 截去尾後的數字 5 得 1234
2. 從 1234 減去 5 的 2 倍 (即 10) 得 1224
3. 從 1224 截去末端的數字 4 得 122
4. 從 122 減去 4 的 2 倍 (即 8) 得 114
5. 從 114 割去末端的數字 4 得 11
6. 從 11 減去 4 的 2 倍 (即 8) 得 3
7. 顯然 3 不是 7 的倍數，可以得知 12345 不能被 7 整除。

$$\begin{array}{rccccc} & 1 & 2 & 3 & 4 & 5 \\ -) & & & 1 & 0 & \\ \hline & 1 & 2 & 2 & 4 & \\ -) & & & 8 & & \\ \hline & 1 & 1 & 4 & & \\ -) & & 8 & & & \\ \hline & & 3 & & & \end{array}$$

例(2): 判定 166712 能否被 7 整除

1. 將原來的數字 166712 截去尾後的數字 2 得 16671
2. 從 16671 減去 4 得 16667
3. 從 16667 截去尾後的數字 7 得 1666
4. 從 1666 減去 14 得 1652
5. 從 1652 截去尾後的數字 2 得 165
6. 從 165 減去 4 得 161
7. 從 161 截去尾後的數字 1 得 16
8. 從 16 減去 2 得 14
9. 顯然 14 能被 7 整除，所以可以得知 166712 能被 7 整除。

$$\begin{array}{rcccccc} & 1 & 6 & 6 & 7 & 1 & 2 \\ -) & & & & & 4 & \\ \hline & 1 & 6 & 6 & 6 & 7 & \\ -) & & & 1 & 4 & & \\ \hline & 1 & 6 & 5 & 2 & & \\ -) & & & 4 & & & \\ \hline & 1 & 6 & 1 & & & \\ -) & & 2 & & & & \\ \hline & 1 & 4 & & & & \end{array}$$

尚有其他數字整除性的檢驗方法，讀者可以在以下的網頁找到：

http://mathsgreat.com/divisibility.html

5.2 "趣味數論"介紹的方法

單墫先生在他的"單墫老師教你學數學：趣味數論"一書中，介紹了一個"因數分解的妙法"，據說這個方法是由美國德雷姆船長設計出來的。以下以 4511, 493 和 23 爲例，演示方法，然後再證明。

5.2.1 示例

例一: 分解 4511(”趣味數論”的示例)

步驟	i	M_i	N_i	
第一步	1	$M_1 = 4511$	$N_1 = 4511$	$4511 = 3 \times 1503 + 2$
第二步	2	$M_2 = 4511 - 2 \times 1503 = 1505$	$N_2 = 1505 + 2 = 1507$	$1507 = 5 \times 301 + 2$
第三步	3	$M_3 = 1505 - 2 \times 301 = 903$	$N_3 = 903 + 2 = 905$	$905 = 7 \times 129 + 2$
第四步	4	$M_4 = 903 - 2 \times 129 = 645$	$N_4 = 645 + 2 = 647$	$647 = 9 \times 71 + 8$
第五步	5	$M_5 = 645 - 2 \times 71 = 503$	$N_5 = 503 + 8 = 511$	$511 = 11 \times 46 + 5$
第六步	6	$M_6 = 503 - 2 \times 46 = 411$	$N_5 = 411 + 5 = 416$	$416 = \mathbf{13} \times 32 + 0$
第七步	7	$M_7 = 411 - 2 \times 32 = 347$		
		每一步的 M 值爲上一步的 M 值減去 2 乘以上一步最右欄綠色的數字	每一步的 N 值爲同一步的 M 值加上一步最右欄藍色的數字	每一步帶餘除法中的除數依次爲 3,5,7,9,11,$\cdots$

其中， $4511 = 13 * 347$。

例二: 分解 493

步驟	i	M_i	N_i	
第一步	1	$M_1 = 493$	$N_1 = 493$	$493 = 3 \times 164 + 1$
第二步	2	$M_2 = 493 - 2 \times 164 = 165$	$N_2 = 165 + 1 = 166$	$166 = 5 \times 33 + 1$
第三步	3	$M_3 = 165 - 2 \times 33 = 99$	$N_3 = 99 + 1 = 100$	$100 = 7 \times 14 + 2$
第四步	4	$M_4 = 99 - 2 \times 14 = 71$	$N_4 = 71 + 2 = 73$	$73 = 9 \times 8 + 1$
第五步	5	$M_5 = 71 - 2 \times 8 = 55$	$N_5 = 55 + 1 = 56$	$56 = 11 \times 5 + 1$
第六步	6	$M_6 = 55 - 2 \times 5 = 45$	$N_6 = 45 + 1 = 46$	$46 = 13 \times 3 + 7$
第七步	7	$M_7 = 45 - 2 \times 3 = 39$	$N_7 = 39 + 7 = 46$	$46 = 15 \times 3 + 1$
第八步	8	$M_8 = 39 - 2 \times 3 = 33$	$N_8 = 33 + 1 = 34$	$34 = \mathbf{17} \times 2 + 0$
第九步	9	$M_9 = 33 - 2 \times 2 = \mathbf{29}$		

其中， $493 = 17 * 29$。

例三: 分解 23

步驟	i	M_i	N_i	
第一步	1	$M_1 = 23$	$N_1 = 23$	$23 = 3 \times 7 + 2$
第二步	2	$M_2 = 23 - 2 \times 7 = 9$	$N_2 = 9 + 2 = 11$	$11 = 5 \times 2 + 1$
第三步	3	$M_3 = 9 - 2 \times 2 = 5$	$N_3 = 5 + 1 = 6$	$6 = 7 \times 0 + 6$
第四步	4	$M_4 = 5 - 2 \times 0 = 5$	$N_4 = 5 + 6 = 11$	$11 = 9 \times 1 + 2$
第五步	5	$M_5 = 5 - 2 \times 1 = 3$	$N_5 = 3 + 2 = 5$	$5 = 11 \times 0 + 5$

第六步	6	$M_6 = 3 - 2 \times 0 = 3$	$N_6 = 3 + 5 = 8$	$8 = 13 \times 0 + 8$
第七步	7	$M_7 = 3 - 2 \times 0 = 3$	$N_7 = 3 + 8 = 11$	$11 = 15 \times 0 + 11$
第八步	8	$M_8 = 3 - 2 \times 0 = 3$	$N_8 = 3 + 11 = 14$	$14 = 17 \times 0 + 14$
第九步	9	$M_9 = 3 - 2 \times 0 = 3$	$N_9 = 3 + 14 = 17$	$17 = 19 \times 0 + 17$
第十步	10	$M_{10} = 3 - 2 \times 0 = 3$	$N_{10} = 3 + 17 = 20$	$20 = 21 \times 0 + 20$
第11步	11	$M_{11} = 3 - 2 \times 0 = 3$	$N_{11} = 3 + 20 = 23$	$23 = \mathbf{23} \times 1$
第12步	12	$M_{12} = 3 - 2 \times 1 = \mathbf{1}$		

其中， $23 = 23 * 1$。

從以上的幾個示例中,可以知道,用這方法來要分解一個小的數並不一定比分解一個大的數快,分解 23 需用上 12 步, 而分解 4511 只需用 7 步。

5.2.2 證明

現將上述的方法再演示一次, 以 Q_i, R_i 分別表示在第 i 步進行帶餘除法時所得的商和餘數, 其中第 i 步帶餘除法的除數是 $2i + 1$。

步驟	i	M_i	N_i	
1	1	M_1	$N_1 = M_1$	$N_1 = 3Q_1 + R_1$
2	2	$M_2 = M_1 - 2Q_1$	$N_2 = M_2 + R_1$	$N_2 = 5Q_2 + R_2$
3	3	$M_3 = M_2 - 2Q_2$	$N_3 = M_3 + R_2$	$N_3 = 7Q_3 + R_3$
$\cdots$		$\cdots$	$\cdots$	$\cdots$
k	k	$M_k = M_{k-1} - 2Q_{k-1}$	$N_k = M_k + R_{k-1}$	$N_k = (2k+1)Q_k + R_k$
$\cdots$		$\cdots$	$\cdots$	$\cdots$
$n-1$	$n-1$	$M_{n-1} = M_{n-2} - 2Q_{n-2}$	$N_{n-1} = M_{n-1} + R_{n-2}$	$N_{n-1} = (2n-1)Q_{n-1} + R_{n-1}$
n	n	$M_n = M_{n-1} - 2Q_{n-1}$	$N_n = M_n + R_{n-1}$	$N_n = (2n+1)Q_n + 0$
$n+1$	$n+1$	$M_{n+1} = M_n - 2Q_n$		

其中， $M_1 = (2n+1)M_{n+1}$。

在上述的算法中,M_k, N_k, Q_k, R_k 有以下的關係:

1. $M_1 = N_1$
2. $N_k = (2k+1) \times Q_k + R_k$
3. 對於 $k \geq 2$, $M_k = M_{k-1} - 2 \times Q_{k-1}$

4. 對於 $k \geq 2, \quad N_k = M_k + R_{k-1}$

由

1. $N_2 = M_2 + R_1$
2. $N_2 = M_1 - 2Q_1 + R_1$
3. $N_2 = M_1 - 5Q_1 + 3Q_1 + R_1$
4. $N_2 = N_1 - 5Q_1 + N_1$

有 (1) $N_2 = 2N_1 - 5Q_1$

因爲

1. $N_3 = M_3 + R_2$
2. $N_3 = M_2 - 2Q_2 + R_2$
3. $N_3 = M_1 - 2Q_1 - 2Q_2 + R_2$
4. $N_3 = N_1 - 2Q_1 - 2Q_2 + N_2 - 5Q_2$
5. $N_3 = N_1 - 2Q_1 - 2Q_2 + (2N_1 - 5Q_1) - 5Q_2$

所以有 (2) $N_3 = 3N_1 - 7(Q_1 + Q_2)$

又因爲

1. $N_4 = M_4 + R_3$
2. $N_4 = M_3 - 2Q_3 + R_3$
3. $N_4 = M_2 - 2Q_2 - 2Q_3 + R_3$
4. $N_4 = M_1 - 2Q_1 - 2Q_2 - 2Q_3 + (N_3 - 7Q_2)$

所以有 (3) $N_4 = 4N_1 - 9(Q_1 + Q_2 + Q_3)$

並可以推出,

$N_k = kN_1 - (2k+1)(Q_1 + Q_2 + \cdots + Q_{k-1})$

上述的結果,可以用數學歸納法證明得到。

在上述算法的第 n 步，因爲 $N_n = nN_1 - (2n+1)(Q_1 + Q_2 + \cdots + Q_{n-1})$, 若 N_n 爲 $2n+1$ 整除，則 $2n+1$ 整除 nN_1, 因爲 n, $2n+1$ 只有公因數 1 ，所以 $2n+1$整除 N_1。（稱 n, $2n+1$ 稱爲互質,爲甚麼 n, $2n+1$ 沒有其他公因數,在稍後部分會再作介紹）

因爲

1. $N_n = (2n+1)Q_n = nN_1 - (2n+1)(Q_1 + Q_2 + \cdots + Q_{n-1}$

2. $M_{n+1} = M_n - 2Q_n = \cdots = M_1 - 2(Q_1 + Q_2 + \cdots + Q_{n-1} + Q_n)$

3. $M_{n+1} = M_1 - 2 \times \dfrac{nN_1 - (2n+1)Q_n}{2n+1} - 2Q_n$

4. $M_{n+1} = M_1 - \dfrac{2nM_1}{2n+1} + 2Q_n - 2Q_n$

5. $M_{n+1} = \dfrac{(2n+1)M_1 - 2nM_1}{2n+1}$

6. $M_{n+1} = \dfrac{M_1}{2n+1}$

所以有 $M_1 = (2n+1) \times M_{n+1}$。

5.3 費馬的因數分解法

數學家費馬亦發明了一個因數分解的方法,先以以下三個示例展示其方法。爲方便起見,先作一個由 1 至 100 的平方之數表,用這個表便可以將任何一個在給定範圍內的奇數分解。

	1	2	3	4	5	6	7	8	9	10
0	1	4	9	16	25	36	49	64	81	100
1	121	144	169	196	225	256	289	324	361	400
2	441	484	529	576	625	676	729	784	841	900
3	961	1024	1089	1156	1225	1296	1369	1444	1521	1600
4	1681	1764	1849	1936	2025	2116	2209	2304	2401	2500
5	2601	2704	2809	2916	3025	3136	3249	3364	3481	3600
6	3721	3844	3969	4096	4225	4356	4489	4624	4761	4900
7	5041	5184	5329	5476	5625	5776	5929	6084	6241	6400
8	6561	6724	6889	7056	7225	7396	7569	7744	7921	8100
9	8281	8464	8649	8836	9025	9216	9409	9604	9801	10000

5.3.1 示例

例一. 分解 2627

1. 找一個僅大於或等於 $\sqrt{2627}$ 的 $x_1, x_1 = 52,\ x_1^2 = 2704$

2. 計算 $x_1^2 - 2627 = 2704 - 2627 = 77 = (y_1)^2$, 77 不是完全平方, $x_2 = x_1 + 1 = 53$

3. $x_2^2 - 2627 = 53^2 - 2627 = 182 = (y_2)^2$, 182 不是完全平方, $x_3 = x_2 + 1 = 54$
4. $x_3^2 - 2627 = 54^2 - 2627 = 289 = (y_3)^2$, 289 是完全平方, $y_3 = 17$
5. 所以 $54^2 - 2627 = 17^2,\ 2627 = 54^2 - 17^2$
6. $2627 = (54 + 17) \times (54 - 17)$
7. $2627 = 71 \times 37$

例二. 分解 5293

1. 找一個僅大於或等於 $\sqrt{5293}$ 的 $x_1, x_1 = 73,\ x_1^2 = 5329$
2. $x_1^2 - 5293 = 5329 - 5293 = 36 = (y_1)^2$, 36 是完全平方
3. 所以 $73^2 - 5293 = 36 = 6^2,\ 5293 = 73^2 - 6^2$
4. $5293 = (73 + 6) \times (73 - 6)$
5. $5293 = 79 \times 67$

例三. 分解 799

1. 找一個僅大於或等於 $\sqrt{799}$ 的 $x - 1, x_1 = 29,\ x_1^2 = 841$
2. $x_1^2 - 799 = 841 - 799 = 45$, 45 不是完全平方, $x_2 = x_1 + 1 = 30$
3. $30^2 - 799 = 900 - 799 = 101$, 101 不是完全平方, $x_3 = x_2 + 1 = 31$
4. $31^2 - 799 = 961 - 799 = 162$, 162 不是完全平方, $x_4 = x_3 + 1 = 32$
5. $32^2 - 799 = 1024 - 799 = 225 = 15^2$
6. $32^2 - 799 = 15^2$
7. $799 = 32^2 - 15^2 = (32 + 15) \times (32 - 15)$
8. $799 = 47 \times 17$

簡單來說,費馬的因數分解一個奇數 N 的方法如下:

1. 找一個僅大於或等於 $\sqrt{N}$ 的整數 x_1,若 $\sqrt{N} = x_1$,N 爲完全平方, $N = x_1 \times x_1$。
2. 若 N 不是完全平方,
   - 計算 $x_1^2 - N$, 若 $x_1^2 - N$ 爲完全平方 y_1^2, 便可用平方差公式, 將 N 分解, 若 $x_1^2 - N$ 不是完全平方, $x_2 = x_1 + 1$

- 計算 $x_2^2 - N$, 若 $x_2^2 - N$ 爲完全平方 y_2^2, 便可用平方差公式, 將 N 分解, 若 $x_2^2 - N$ 不是完全平方, $x_3 = x_2 + 1$
- $\cdots$
- 重複以上步驟,直到得到 $x_k^2 - N$ 爲完全平方爲止,其中 $x_k = x_{k-1} + 1$。再用平方差公式,便可以將 N 分解。

5.3.2 費馬分解法的基礎

費馬的分解法建基於以下幾點:

1. 每一個奇數皆可表成平方差
2. 需以僅大於 $\sqrt{N}$ 的整數作起點
3. 只需有限個步驟

1.每一個奇數皆可表成平方差

1. 設給定的奇數爲 N,
2. 若 N 爲質數, $N = N \times 1$,
   若 N 爲合成數, $N = a \times b$, 其中 a, b皆爲奇數。
3. 所以, N 可以表爲兩個奇數(包括 1) a, b 的乘積,不失其一般性,設 $a > b$。
4. $N = a \times b = (\frac{a+b}{2} + \frac{a-b}{2}) \times (\frac{a+b}{2} + \frac{a-b}{2})$,
   因爲 a, b是奇數, 所以$a+b, a-b$ 是正的偶數, 而 $\frac{a+b}{2}, \frac{a-b}{2}$爲正整數。
5. 所以有 $N = (\frac{a+b}{2})^2 - (\frac{a-b}{2})^2$

2. 需以僅大於 $\sqrt{N}$ 的整數作起點

1. 若 $N = x^2 - y^2$
2. $x^2 = N + y^2$
3. $x^2 > N$
4. $\therefore x > \sqrt{N}$

3. 只需有限個步驟

基本上, 費馬的分解法是以試誤的方法找尋兩個平方,使得要被分解的數可以表爲平方差。問題是,是否需要無止境的試? 答案是,不需要!!

1. $\because N = x^2 - y^2 = (x+y)(x-y), \quad x > y$
2. $N > x + y$
3. 假設在第 $k, k+1$ 次試誤時分別有

$$\begin{aligned} x_k^2 - N &= y_k^2 \\ x_{k+1}^2 - N &= y_{k+1}^2 \\ \therefore x_{k+1}^2 - x_k^2 &= y_{k+1}^2 - y_k^2 \end{aligned}$$

4. $\because x_{k+1}, x_k$爲正整數 ,且設 y_{k+1}, y_k爲正數, 有

$$\begin{aligned} y_{k+1}^2 - y_k^2 &= x_{k+1}^2 - x_k^2 > 0 \\ \therefore y_{k+1} &> y_k \\ x_{k+1} + y_{k+1} &> x_k + y_k \end{aligned}$$

5. 因爲 $N > x_k + y_k$, 所以, 若在第 k 次試誤時,$x_k + y_k \geq N$,試誤便可終止。

例. 分解 45

1. 找一個僅大於 $\sqrt{45}$ 的 $x, x = 7$
2. $7^2 - 45 = 4$
3. $45 = 7^2 - 2^2$
   $45 = (7+2)(7-2) = 9 \times 5$; 但是 45 還可以表爲其他數的乘積嗎?
4. $8^2 - 45 = 64 - 45 = 19,$
5. $9^2 - 45 = 81 - 45 = 36,$
   $45 = 9^2 - 6^2 = 15 \times 3$
6. $10^2 - 45 = 100 - 23 = 41,$
7. $11^2 - 45 = 76, \ \cdots$
8. $23^2 - 45 = 529 - 45 = 484 = 22^2, \quad 45 = 23^2 - 22^2 = 45 \times 1$
9. 所以, 45 可分解成 (1) 9×5, (2) 15×3, 和 (3) 45×1,

觀察上述的示例，可以得知對於任何奇數 N,當試誤的 $x_k = \frac{N+1}{2}$時，有

$$
\begin{aligned}
y_k^2 &= (\frac{N+1}{2})^2 - N \\
y_k^2 &= \frac{N^2+2N+1}{4} - N \\
y_k^2 &= \frac{N^2+2N+1-4N}{4} \\
y_k &= \frac{N-1}{2} \\
N &= (\frac{N+1}{2} + \frac{N-1}{2})(\frac{N+1}{2} - \frac{N-1}{2})
\end{aligned}
$$

因爲，$x_k + y_k = \frac{N+1}{2} + \frac{N-1}{2} = N$, 試誤便可以終止。

用費馬的因數分解方法來檢定一個數是否爲質數並不是一個好的方法，以 101 爲例，試誤的起步點爲 11，而需要試到 $x_k = 51$ 時停止，方可確定除了 101×1 以外，101 不能表示爲兩個奇數的乘積，而後才能判定 101 爲質數。